Einige Bemerkungen über die Tschirnhaussche Transformation von Polynomidealen

Von WILFRIED NÖBAUER in Wien

L. RÉDEI hat in seinem Buch [1] die Tschirnhaussche Transformation von Idealen eines Polynomringes in einer Unbestimmten definiert und einige Aussagen darüber gewonnen. Diesen Begriff wollen wir auf Polynomideale in n Unbestimmten verallgemeinern und weitere einfache Sätze darüber beweisen. Insbesondere werden wir sehen, daß er in einem gewissen Zusammenhang steht mit dem von mir eingeführten Begriff des Vollideales (vergleiche [2]).

Es sei ϱ ein kommutativer Ring mit Einselement und $R = \varrho[x_1, x_2, \ldots, x_n]$. Wir bilden die direkte Summe von n Exemplaren von R und bezeichnen sie mit R_n, die Elemente von R_n denken wir uns in Komponentenschreibweise geschrieben. Sind

$$\mathfrak{a} = (f_1(x_1 \ldots x_n), f_2(x_1 \ldots x_n), \ldots, f_n(x_1 \ldots x_n)),$$
$$\mathfrak{b} = (g_1(x_1 \ldots x_n), g_2(x_1 \ldots x_n), \ldots, g_n(x_1 \ldots x_n))$$

zwei Elemente von R_n, so definieren wir für sie die Verknüpfung „Komposition" — wir drücken sie aus durch das Zeichen $\circ$ — durch

$$\mathfrak{a} \circ \mathfrak{b} = (f_1(g_1, \ldots, g_n), f_2(g_1, \ldots, g_n), \ldots, f_n(g_1, \ldots, g_n)).$$

In Bezug auf diese Verknüpfung bildet R_n eine Halbgruppe mit dem Einselement $(x_1, x_2, \ldots, x_n) = \mathfrak{x}$.

Es sei nun A ein Ideal in R und $\mathfrak{t} = (t_1, t_2, \ldots, t_n)$ ein Element von R_n. Man erkennt sofort, daß gilt:

Die Menge aller Polynome $k(x_1, x_2, \ldots, x_n) \in R$ mit $k(\mathfrak{t}) = k(t_1, t_2, \ldots, t_n) \in A$ bildet ein Ideal in R, das mit $A^{\mathfrak{t}}$ bezeichnet sei.

Wir sagen, daß $A^{\mathfrak{t}}$ aus A durch die Tschirnhaussche Transformation mit $\mathfrak{t}$ hervorgeht.

Im Fall $n = 1$ geht unsere Definition ersichtlich in die von RÉDEI gegebene über.

Wir wollen zunächst einige Rechenregeln für die Bildung der Tschirnhaus-Transformierten von Idealen A zusammenstellen. Es gilt:

(1) $$(A^{\mathfrak{t}})^{\mathfrak{u}} = A^{\mathfrak{u} \circ \mathfrak{t}}.$$

Beweis. $f(\mathfrak{x}) \in (A^{\mathfrak{t}})^{\mathfrak{u}} \leftrightarrow f(\mathfrak{u}) \in A^{\mathfrak{t}} \leftrightarrow f(\mathfrak{u} \circ \mathfrak{t}) \in A \leftrightarrow f(\mathfrak{x}) \in A^{\mathfrak{u} \circ \mathfrak{t}}$.

Weiter haben wir:

(2) Aus $A \subseteqq B$ folgt stets $A^{\mathfrak{t}} \subseteqq B^{\mathfrak{t}}$.

Das ist unmittelbar einzusehen.

Daß aber aus $A \subset B$ nicht $A^t \subset B^t$ folgen muß, erkennt man an folgendem Beispiel:

Es sei $n=1$, ϱ der Ring der ganzen Zahlen, $A=(0)$, $B=(x)$ und $t=0$. Dann gilt:

$$A^t=(x),\quad B^t=(x),\quad \text{aber}\quad A \subset B.$$

Für eine beliebige Indexmenge $\{\nu\}$ bezeichnen wir wie üblich mit $\bigcap_\nu A_\nu$ den Durchschnitt der Ideale A_ν, mit $\sum_\nu A_\nu$ das von der Vereinigungsmenge der A_ν erzeugte Ideal. Falls $\{\nu\}$ endlich ist, dann bezeichnen wir mit $\prod_\nu A_\nu$ das vom Komplexprodukt der A_ν erzeugte Ideal. Es gilt:

$$(3)\qquad \Big(\bigcap_\nu A_\nu\Big)^t=\bigcap_\nu A_\nu^t,$$

$$(4)\qquad \Big(\sum_\nu A_\nu\Big)^t \supseteq \sum_\nu A_\nu^t,$$

$$(5)\qquad \Big(\prod_\nu A_\nu\Big)^t \supseteq \prod_\nu A_\nu^t.$$

Wir beweisen diese Beziehungen folgendermaßen:

$$f(\mathfrak{x}) \in \Big(\bigcap_\nu A_\nu\Big)^t \;\rightarrow\; f(\mathfrak{t}) \in \bigcap_\nu A_\nu \;\rightarrow\; f(\mathfrak{t}) \in A_\nu \text{ für jedes } \nu \;\rightarrow$$

$$\rightarrow\; f(\mathfrak{x}) \in A_\nu^t \text{ für jedes } \nu \;\rightarrow\; f(\mathfrak{x}) \in \bigcap_\nu A_\nu^t;$$

$$f(\mathfrak{x}) \in \sum_\nu A_\nu^t \;\rightarrow\; f(\mathfrak{x}) = \sum_{i=1}^{r} g_{\nu_i}(\mathfrak{x}) \text{ mit } g_{\nu_i}(\mathfrak{x}) \in A_{\nu_i}^t \;\rightarrow$$

$$\rightarrow\; f(\mathfrak{t}) = \sum_{i=1}^{r} g_{\nu_i}(\mathfrak{t}) \;\rightarrow\; f(\mathfrak{t}) \in \sum_\nu A_\nu \;\rightarrow\; f(\mathfrak{x}) \in \Big(\sum_\nu A_\nu\Big)^t;$$

$$f(\mathfrak{x}) \in \prod_\nu A_\nu^t \;\rightarrow\; f(\mathfrak{x}) = \sum g_1(\mathfrak{x}) g_2(\mathfrak{x}) \ldots g_r(\mathfrak{x}) \text{ mit } g_i(\mathfrak{x}) \in A_i^t \;\rightarrow$$

$$\rightarrow\; f(\mathfrak{t}) = \sum g_1(\mathfrak{t}) g_2(\mathfrak{t}) \ldots g_r(\mathfrak{t}) \;\rightarrow\; f(\mathfrak{t}) \in \prod_\nu A_\nu \;\rightarrow\; f(\mathfrak{x}) \in \Big(\prod_\nu A_\nu\Big)^t.$$

Es läßt sich aber weder in (4) noch in (5) das $\subseteq$ Zeichen durch das Zeichen $=$ ersetzen, wie man an folgenden Beispielen erkennt:

Es sei $n=1$, ϱ der Ring der ganzen Zahlen und $\{\nu\}=\{1,2\}$. Wir nehmen $A_1=(x)$, $A_2=(x+1)$ und $t=0$. Dann erhalten wir:

$$A_1^t=(x),\quad A_2^t=(x).$$

Wir haben $\sum_\nu A_\nu = (x, x+1) = R$, daher $\big(\sum_\nu A_\nu\big)^t = R$, weshalb hier in (4) nicht das Gleichheitszeichen gilt.

Weiter haben wir $\prod_\nu A_\nu = (x(x+1))$, daher $\big(\prod_\nu A_\nu\big)^t = (x)$, weshalb hier auch in (5) nicht das Gleichheitszeichen gilt.

Wir bezeichnen das Ideal $A \subseteqq R$ als Vollideal, wenn gilt: *Aus* $f(\mathfrak{x}) \in A$ *folgt* $f(\mathfrak{t}) \in A$ *für jedes* $\mathfrak{t} \in R_n$.

Wir beweisen folgenden

Satz. *Ist A Ideal in R, dann ist das Ideal* $\bigcap_{\mathfrak{r} \in R_n} A^{\mathfrak{r}}$ *Vollideal von R, welches in A enthalten ist und alle in A enthaltenen Vollideale umfaßt.*

$\bigcap_{\mathfrak{r} \in R_n} A^{\mathfrak{r}}$ ist also das „größte" in A enthaltene Vollideal.

Beweis. Wir setzen $\bigcap_{\mathfrak{r} \in R_n} A^{\mathfrak{r}} = D$. Wegen $A^{\mathfrak{x}} = A$ haben wir $D \subseteqq A$. Daß D Vollideal ist, sieht man folgendermaßen ein: Sei $f(\mathfrak{x}) \in D$ und $\mathfrak{t} \in R_n$ sowie $\mathfrak{r} \in R_n$. Dann haben wir

$$f(\mathfrak{x}) \in A^{\mathfrak{t} \circ \mathfrak{r}} = (A^{\mathfrak{r}})^{\mathfrak{t}},$$

daher gilt $f(\mathfrak{t}) \in A^{\mathfrak{r}}$, woraus sich, da $\mathfrak{r}$ beliebig sein kann, sogleich $f(\mathfrak{t}) \in D$ ergibt. Ist schließlich $V \subseteqq A$ Vollideal von R, so folgt aus $f(\mathfrak{x}) \in V$ stets $f(\mathfrak{x}) \in V \subseteqq A$, also gilt $V \subseteqq A^{\mathfrak{r}}$, also $V \subseteqq D$.

Aus dem Satz erhalten wir sogleich folgendes

Korollar. *Das Ideal A von R ist dann und nur dann Vollideal, wenn gilt* $A = \bigcap_{\mathfrak{r} \in R_n} A^{\mathfrak{r}}$.

Bemerkung. Die Tschirnhaustransformierte $A^{\mathfrak{r}}$ eines Vollideales A braucht keineswegs wieder ein Vollideal zu sein. Dies erkennt man etwa an folgendem Beispiel:

ϱ sei der Ring der ganzen Zahlen und $n = 1$. Es sei $A = (2)$ (das ist ersichtlich ein Vollideal) und $\mathfrak{t} = 0$. Dann haben wir $A^{\mathfrak{t}} = (x, 2)$, was ersichtlich kein Vollideal ist.

Eine naheliegende, aber anscheinend nur schwer zu beantwortende Frage ist folgende: Wie kann man ein vollständiges System der verschiedenen Tschirnhaustransformierten eines gegebenen Ideales A erhalten?

In Zusammenhang mit dieser Frage zeigen wir zunächst:

Das Einheitsideal R ist das einzige Ideal, das mit allen seinen Tschirnhaustransformierten übereinstimmt.

Beweis. Daß stets $R^{\mathfrak{r}} = R$ gilt, ist klar. Sei andererseits $A^{\mathfrak{r}} = A$ für alle $\mathfrak{r} \in R_n$; nach dem vorhin bewiesenen Satz ist dann A ein Vollideal, mit $f(x_1, x_2 \dots x_n) \in A$ gilt also für beliebige $u_i \in \varrho$ auch $f(u_1, u_2 \dots u_n) \in A$. Da auch für das Nullelement $\mathfrak{o} \in R_n$ gilt $A^{\mathfrak{o}} = A$, gehört jedes Polynom, dessen konstantes Glied zu A gehört, schon zu A, also haben wir insbesondere $x_1 \in A$, nach dem vorher festgestellten also $e \in A$ für das Einselement e von ϱ, also gilt $A = R$.

Für ein beliebiges Ideal A von R bezeichnen wir mit A_n diejenigen Elemente von R_n, deren sämtliche Komponenten zu A gehören. Klarerweise ist A_n ein Ideal in R_n und man erkennt sofort, daß in Verallgemeinerung einer Bemerkung von [1] gilt: Aus $\mathfrak{r} \equiv \mathfrak{d} \bmod A_n$ folgt stets $A^{\mathfrak{r}} = A^{\mathfrak{d}}$. Bezeichnet man also die Restklasse von $\mathfrak{r} \bmod A_n$ mit $\bar{\mathfrak{r}}$, so ist stets $A^{\bar{\mathfrak{r}}}$ ein eindeutig bestimmtes Ideal. Ist insbesondere R/A endlich, so hat A nur endlich viele verschiedene Tschirnhaustransformierte.

Setzt man voraus, daß A Vollideal ist, so ist die Kongruenzrelation mod A_n auch eine Kongruenzrelation in der von R_n in Bezug auf die Verknüpfung Komposition

gebildeten Halbgruppe (siehe [2]) und man kann die Faktorhalbgruppe R_n/A_n nach dieser Kongruenzrelation bilden, deren Elemente eben die Restklassen $\bar{\mathfrak{r}}$ mod A_n sind. Wir zeigen für diesen Fall:

Genau dann gilt $A^{\bar{\mathfrak{r}}} = A$, wenn $\bar{\mathfrak{r}}$ ein rechtsreguläres Element der Faktorhalbgruppe R_n/A_n ist.

Beweis. Sei $\bar{\mathfrak{r}}$ rechtsregulär. Da A Vollideal ist, gilt für $f(\mathfrak{x}) \in A$ stets $f(\mathfrak{r}) \in A$, also haben wir $A \subseteq A^{\bar{\mathfrak{r}}}$. Ist umgekehrt $f(\mathfrak{x}) \in A^{\bar{\mathfrak{r}}}$, so haben wir $f(\mathfrak{r}) \in A$. Wir bilden das Element

$$\bar{\mathfrak{f}} = (f(\mathfrak{x}), f(\mathfrak{x}), \ldots, f(\mathfrak{x})) \in R_n.$$

Für dieses gilt

$$\bar{\mathfrak{f}} \circ \bar{\mathfrak{r}} = \overline{\mathfrak{f} \circ \mathfrak{r}} = \bar{\mathfrak{v}} = \bar{\mathfrak{v}} \circ \bar{\mathfrak{r}},$$

also $\bar{\mathfrak{f}} = \bar{\mathfrak{v}}$, $f(\mathfrak{x}) \in A$. Daher gilt auch $A^{\bar{\mathfrak{r}}} \subseteq A$.

Sei umgekehrt $A^{\bar{\mathfrak{r}}} = A$. Gilt $\bar{\mathfrak{f}} \circ \bar{\mathfrak{r}} = \bar{\mathfrak{g}} \circ \bar{\mathfrak{r}}$, so haben wir $(\bar{\mathfrak{f}} - \bar{\mathfrak{g}}) \circ \bar{\mathfrak{r}} = \bar{\mathfrak{v}}$, also $(\mathfrak{f} - \mathfrak{g}) \circ \mathfrak{r} \equiv \mathfrak{v} \bmod A_n$. Daraus folgt für alle Komponenten f_i, g_i von $\mathfrak{f}$ bzw. $\mathfrak{g}$

$$f_i - g_i \in A^{\mathfrak{r}} = A,$$

also $\bar{\mathfrak{f}} = \bar{\mathfrak{g}}$, weshalb $\bar{\mathfrak{r}}$ rechtsregulär ist.

Aus diesem Resultat können wir folgern:

Ist A Vollideal und R/A endlich, so gilt $A^{\bar{\mathfrak{r}}} = A$ genau dann, wenn $\bar{\mathfrak{r}}$ ein invertierbares Element der Faktorhalbgruppe R_n/A_n ist.

Beweis. Aus der Endlichkeit von R/A folgt, daß auch R_n/A_n endlich ist. Bezeichnen wir die Menge der rechtsregulären Elemente von R_n/A_n mit $\mathfrak{R}$, die der invertierbaren mit $\mathfrak{J}$, so gilt natürlich $\mathfrak{J} \subseteq \mathfrak{R}$. Andererseits ist $\mathfrak{R}$ eine Unterhalbgruppe von R_n/A_n — das Produkt zweier rechtsregulärer Elemente ist ja wieder stets rechtsregulär — mit der Einheit $\bar{\mathfrak{x}}$; da für $\bar{\mathfrak{r}} \in \mathfrak{R}$ das $\bar{\mathfrak{f}} \circ \bar{\mathfrak{r}}$ zusammen mit $\bar{\mathfrak{f}}$ alle Elemente von R_n/A_n durchläuft, hat $\bar{\mathfrak{r}}$ ein Linksinverses $\bar{\mathfrak{d}}$, und dieses ist, da es ein Rechtsinverses hat, rechtsregulär, gehört also zu $\mathfrak{R}$. Deshalb ist $\mathfrak{R}$ eine Gruppe und es gilt also auch $\mathfrak{R} \subseteq \mathfrak{J}$.

Bezeichnen wir die Unterhalbgruppe der rechtsregulären Elemente von R_n/A_n weiterhin mit $\mathfrak{R}$, so können wir noch sagen:

Wenn zwei Elemente von R_n/A_n zur selben Linksnebenklasse nach $\mathfrak{R}$ gehören, dann ergeben sie dieselbe Tschirnhaustransformierte von A.

Beweis. Es seien $\bar{\mathfrak{d}}$ und $\bar{\mathfrak{t}}$ Elemente von $\bar{\mathfrak{g}} \circ \mathfrak{R}$. Dann haben wir $\bar{\mathfrak{d}} = \bar{\mathfrak{g}} \circ \bar{\mathfrak{r}}_1$ und $\bar{\mathfrak{t}} = \bar{\mathfrak{g}} \circ \bar{\mathfrak{r}}_2$, daraus folgt $A^{\bar{\mathfrak{d}}} = A^{\bar{\mathfrak{g}}} = A^{\bar{\mathfrak{t}}}$.

Daß sich der soeben bewiesene Satz aber nicht umkehren läßt, also auch Elemente aus verschiedenen Linksnebenklassen von R_n/A_n dieselbe Tschirnhaustransformierte von A ergeben können, zeigt folgendes Beispiel:

Es sei $n = 1$ und ϱ das Galoisfeld mit den drei Elementen $\bar{0}, \bar{1}, \bar{2}$. A sei das Ideal $(x^3 - x)$, das ist ein Vollideal, denn es besteht aus den für alle Werte aus ϱ verschwindenden Polynomen. Man erkennt leicht, daß $R_n/A_n = R/A$ endlich ist und isomorph

zur Halbgruppe $\mathfrak{F}_3$ aller eindeutigen Abbildungen von ϱ in sich. $\mathfrak{N}$ ist daher isomorph zur Gruppe der invertierbaren Elemente von $\mathfrak{F}_3$, das ist die Gruppe $\mathfrak{S}_3$ aller Permutationen der Elemente von ϱ. Wir betrachten nun Polynome $f_1(x)$ und $f_2(x)$, die den Abbildungen $\begin{pmatrix}\bar{0}&\bar{1}&\bar{2}\\ \bar{0}&\bar{0}&\bar{1}\end{pmatrix}$ bzw. $\begin{pmatrix}\bar{0}&\bar{1}&\bar{2}\\ \bar{0}&\bar{1}&\bar{1}\end{pmatrix}$ entsprechen. Wie man sofort erkennt, liegen diese Abbildungen in verschiedenen Linksnebenklassen von $\mathfrak{F}_3$ nach $\mathfrak{S}_3$, also liegen $\overline{f_1(x)}$ und $\overline{f_2(x)}$ in verschiedenen Linksnebenklassen nach $\mathfrak{N}$. Wir haben aber

$$A^{\overline{f_1(x)}} = A^{\overline{f_2(x)}} = (x^2 - x).$$

Wir wollen schließlich noch ein einfaches Beispiel für ein Ideal geben, das unendlich viele verschiedene Tschirnhaustransformierte hat. Es sei $n=1$, ϱ der Ring der ganzen Zahlen, $A=(0)$. Für $g \in \varrho$ haben wir dann:

$$A^g = (x-g)$$

wir erhalten also tatsächlich unendlich viele verschiedene Tschirnhaustransformierte für A.

Literatur

[1] L. Rédei, *Algebra*. I (Leipzig, 1959).
[2] W. Nöbauer, Die Operation des Einsetzens bei Polynomen in mehreren Unbestimmten, *J. reine angew. Math.*, **201** (1959), 207–220.

(Eingegangen am 29. Juli 1961)